(12) UK Patent Application (19) GB (11) 2 316 278 (13) A

(43) Date of A Publication 18.02.1998

(21) Application No 9616803.4

(22) Date of Filing 09.08.1996

(71) Applicant(s)
Richard Steven Faria
21 Denmark Street, LONDON, WC2H 8NE,
United Kingdom

(72) Inventor(s)
Richard Steven Faria

(74) Agent and/or Address for Service
Carpmaels & Ransford
43 Bloomsbury Square, LONDON, WC1A 2RA,
United Kingdom

(51) INT CL[6]
H04L 9/18

(52) UK CL (Edition P)
H4P PDCST

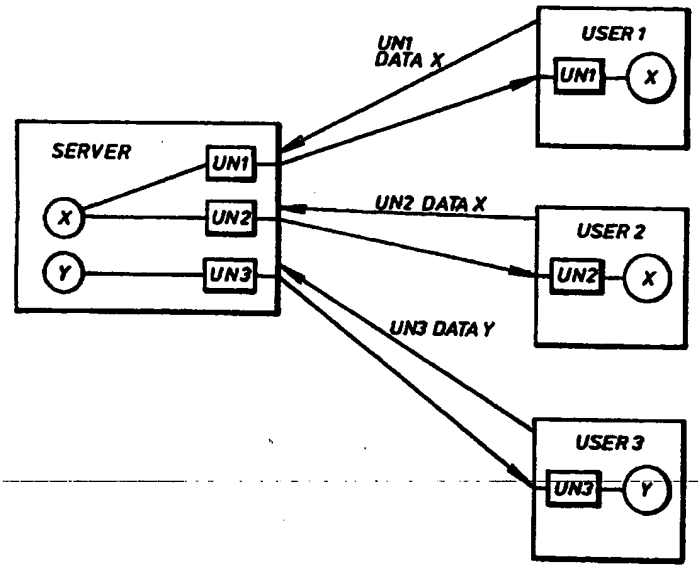
(56) Documents Cited
US 5544161 A US 5477263 A
Data Communications,Computer networks and Open Systems by Fred Halsall 3rd Ed 1992 pp 588-593

(58) Field of Search
UK CL (Edition O) H4P PDCSA PDCSL PDCSP PDCST
INT CL[6] H04L 9/18 9/32
Online:WPI

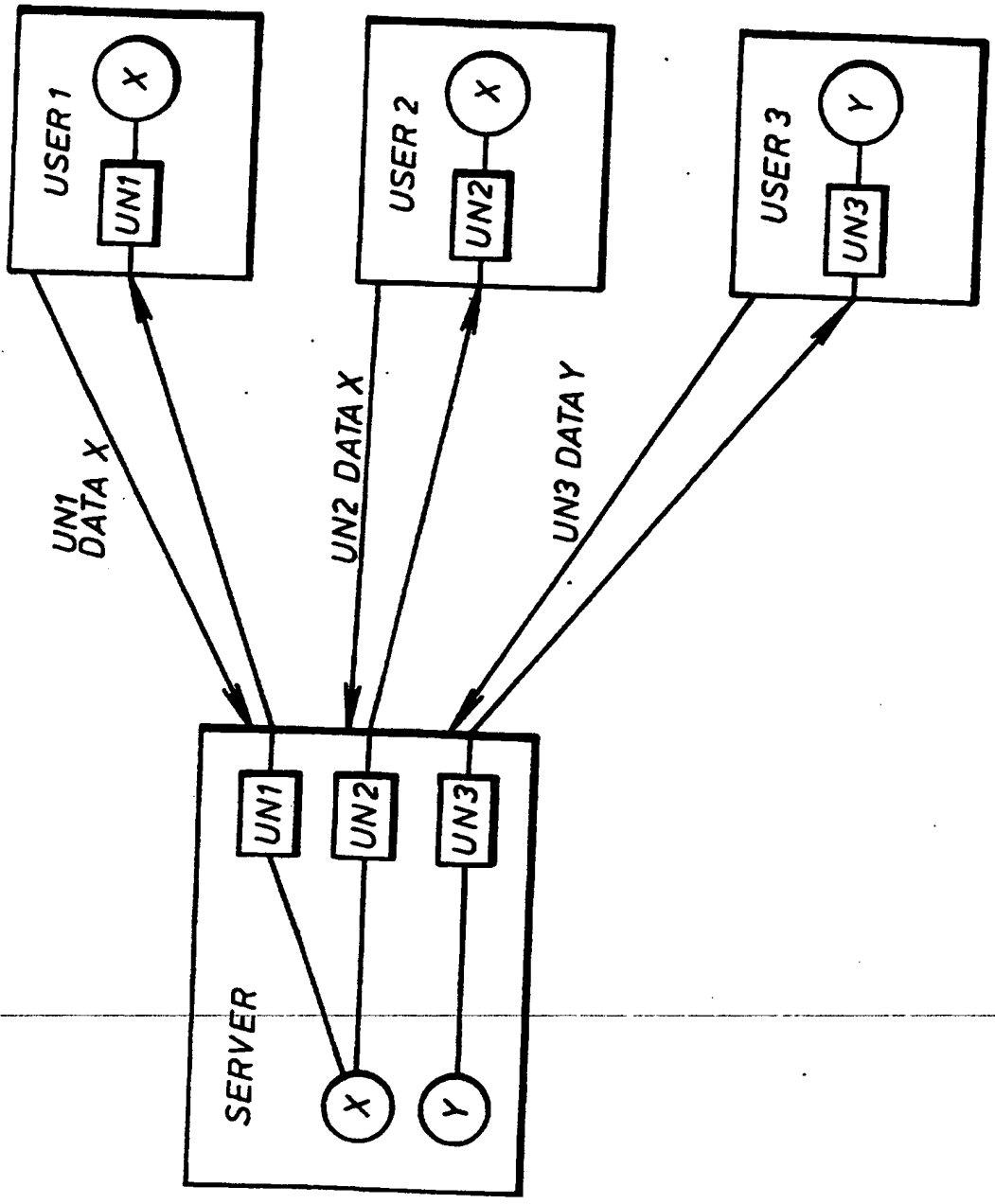
(54) Data Encryption

(57) A method of encrypting digital data to be transmitted comprises transforming each bit of data into a corresponding bit in dependence on an encryption key, in the form of a further bit sequence. A logical exclusive OR function is employed, both to encrypt the data and subsequently for decryption.

This finds particular application in the transmission of MPEG audio and/or video data which may be subject to copyright protection.



GB 2 316 278 A


USER 1
X
UN1
USER 2
X
UN2
USER 3
Y
UN3
UN1 DATA X
UN2 DATA X
UN3 DATA Y
SERVER
UN1
UN2
UN3
X
Y

2316278

DATA ENCRYPTION

The present invention relates to encryption and/or decryption of transmitted data and in particular to transmitted audio and/or video data.

Whenever audio/video data is transmitted from a transmitting station to a receiving station, there is the risk that third parties may also receive the data, and, in the case of data subject to copyright protection, they can prevent copyright owners receiving appropriate renumeration. In the case of such transmission occurring on the Internet, large numbers of people could receive, and therefore benefit from, such data transmission without paying appropriate royalties. To overcome this problem, it has been proposed to encrypt certain parts of the transmitted data with the aim of enabling reception only by authorised receivers, who are provided with means for decrypting the data.

A preferred format for audio data transmission on the Internet is MPEG, as described in ISO IEC 11172-1,2,3,4,5. This format uses a data compression technique to enable large amounts of data to be transmitted for a given bandwidth. Such data is transmitted in data files termed "bitstreams" having four separate sections, namely: (1) a header section containing synchronization and stereo/mono state data; (2) an error check data section containing information regarding error detection; (3) an audio data section containing the audio data which may be subject to copyright protection; and (4) an ancillary data section.

It has been suggested that such data files could be protected against unauthorised reception and redistribution by encrypting the ancillary data section. However, it is feasible for a user to receive such a data file, remove the header and ancillary data sections and to replace them, thereby circumventing the encryption.

Conventional encryption methods are based on an algorithmic transformation of a group of data bits. Such a process is, however, time-consuming, and this is the reason why the audio/video data is not generally encoded.

It would therefore be desirable to provide a method of encryption and/or decryption which overcomes, or at least mitigates, this problem.

In accordance with a first aspect of the present invention there is provided a method of encrypting data in the form of a first sequence of bits into a second sequence of bits, the method comprising individually transforming each bit of said first sequence into a corresponding bit of said second sequence in dependence on an encryption key.

The method extends to a data transmission method incorporating such an encryption method.

In accordance with a further aspect of the present invention there is provided data decryption apparatus comprising means for receiving a sequence of bits representing encrypted data, means for individually transforming each bit of the sequence into a corresponding bit of a further sequence in dependence on an encryption key.

A preferred embodiment of the present invention will now be described with reference to the accompanying drawing which illustrates a transmission system incorporating data encryption and decryption of the preferred embodiment.

A server stores identity codes UN1, UN2, UN3 ... for all authorised users USER 1, USER 2, USER 3 ... of the system. The server also stores audio and/or video data X, Y which may be requested by one or more of the users. When a user, e.g. USER 1, requests transmission of audio data X, it transmits to the server its unique identity code UN1, together with a request for audio data X. The server then encrypts a data file X including audio data X using the identity code UN1 as the encryption key and transmits the encrypted data file to USER 1. USER 1 then decrypts the encrypted data using the encryption key UN1 to regenerate the original data file X including the audio data X. Whilst

it is possible for other users to receive this data, they will not be able to decrypt it, because their respective decryption keys UN2, UN3 ... are different from UN1.

The method of encryption is as follows. Each data bit within the data file X is logically combined as an exclusive OR (XOR) function with a corresponding bit from a bit sequence constituting the user identity code, e.g. UN1. An exclusive OR function is a logical combination having the value 0 if both data bits A and B are the same and the value 1 if they are different:

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

For example, if the audio data X comprises the bit sequence 1001110 ... and the user identity code UN1 comprises the bit sequence 0001101 ..., then the resulting combination would be 1000011 ...

When the user receives the encrypted data, a corresponding decryption method is used, again using an exclusive OR function. Such a function has the property that if the exclusive OR combination C, of two bits A and B is itself combined with one of the two bits, e.g. A, the other bit B is generated:

A	B	A XOR B=C
0	0	0
0	1	1
1	0	1
1	1	0

C	A	C XOR A = B
0	0	0
1	0	1
1	1	0
0	1	1

Thus, in the above example, when the resulting XOR combination is recombined with the user identity code UN1, the original data file X is retrieved, as follows:

Data file X (A)	1001110 ...
User identity code UN1 (B)	0001101 ...
XOR combination of A and B (C)	1000011 ...
User identity code UN1 (B)	0001101 ...
XOR combination of B and C = Data file X	1001110 ...

The user identity code is typically 32 or 64 bits long, and when the last bit of the code has been used the sequence is repeated until all the audio data has been encrypted.

Initially, a user is registered by supplying credit/debit card details to the server, and, once suitable bank checks have been made, the server generates a unique user identity code which is stored in a user's module. When a user requires a data transmission, the user identity code is read from the module and transmitted, along with the data request, to the server. It will be appreciated that the above-described preferred embodiment of the present invention provides a secure method of transmitting data from a server of a user thus preventing unauthorised reception of copyright-protected data. Various modifications of the preferred embodiment may be made without departing from the scope of the invention, which is defined by the following claims.

CLAIMS

1. A method of encrypting data in the form of a first sequence of bits into a second sequence of bits the method comprising individually transforming each bit of said first sequence into a corresponding bit of said second sequence in dependence on an encryption key.

2. A method as claimed in claim 1, wherein said encryption key comprises a third sequence of bits.

3. A method as claimed in claim 2, wherein said encryption key comprises 32 bits.

4. A method as claimed in claim 2, wherein said encryption key comprises 64 bits.

5. A method as claimed in any one of claims 2 to 4, wherein the individual transformation comprises logically combining each bit of said first sequence with a bit selected from said third sequence.

6. A method as claimed in claim 5, wherein the bits of said first and third sequences are so combined using a logical exclusive OR function.

7. A method as claimed in claim 5 or claim 6, wherein the bits of said third sequence are selected sequentially from the first bit in the third sequence to the last bit and wherein the sequential selection is repeated until all bits of the first sequence have been logically combined.

8. A method as claimed in any preceding claim, wherein the first sequence of bits comprises audio or video data within an MPEG bitstream.

9. A method as claimed in claim 8, wherein the first sequence of bits comprises a complete MPEG bitstream.

10. A data transmission method of transmitting data from a server to a user, the method comprising:

receiving from a user a unique identity code and a request for data;

encrypting the requested data in accordance with any preceding claim, wherein the encryption key is a function of the received identity code; and

transmitting the encrypted data to the user.

11. A method as claimed in claim 10, wherein the encryption key is identical to the received identity code.

12. Data decryption apparatus comprising means for receiving a sequence of bits representing encrypted data, means for individually transforming each bit of the sequence into a corresponding bit of a further sequence in dependence on an encryption key.

13. Data decryption apparatus as claimed in claim 12, wherein the encryption key comprises a third sequence of bits, said transforming means comprising means for logically combining each bit of said received sequence with a bit selected from said third sequence.

14. Data decryption apparatus as claimed in claim 13, wherein said combining means comprises a logical exclusive OR gate.

15. A method of encrypting data substantially as hereinbefore described with reference to and as shown in the accompanying drawing.

16. A data transmission method substantially as hereinbefore described with reference to and as shown in the accompanying drawing.

17. Data decryption apparatus substantially as hereinbefore

described with reference to and as shown in the accompanying drawing.

The Patent Office

8

Application No: GB 9616803.4 **Examiner:** Mr B J Spear
Claims searched: 1-17 **Date of search:** 19 November 1996

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.O): H4P (PDCSA, PDCSP, PDCSL, PDCST)

Int Cl (Ed.6): H04L 9/18,9/32

Other: Online: WPI

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
Y	US5544161	(Bell Atlantic) Whole document, eg col. 11 lines 23-41, claims 4 and 9	8,9
Y	US5477263	(Bell Atlantic) Whole document, eg col. 2 lines 12-29, claim 6	8,9
XY	Data Communications, Computer Networks and Open Systems by Fred Halsall, 3rd Ed Pub. Addison-Wesley 1992, ISBN 0-201-56506-4. Pages 588-593.		1-14

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.